1.0 Background:

Call Accounting (CA) is an important function associated with Private Branch Exchange (PBX) telephone systems used within many businesses. In typical applications, CA functionality is provided through use of a CA software package which receives telephone call information, referred to as Call Detail Records (CDR), or tickets, from the PBX. The CA software package processes this CDR data to produce reports in various formats. CA processing includes calculating the cost for each call based on calling number, called number, time of day, trunk, telephone company tariff rates, and other parameters.

CA reports are used by the business enterprise to track the number and cost of calls made by individuals, and departments within each division, and to correctly apportion call costs to the appropriate cost center. CA software packages produce reports in a wide variety of formats, and reports can be automatically scheduled. Typical CA software packages also detect inappropriate usage of the PBX system such as expensive off-hour calls, or trunk-to-trunk calling and provide alerts to the PBX manager via email, paging and other means. Additional functionality found in modern CA software packages includes trunk analysis, so that the number of T1 trunks, connected to the PBX and shared between the many users of the PBX, can be optimized on a continuing basis.

1.1 Enterprise-Resident Call Accounting Architectures:

In many applications, the CA functionality is provided entirely within the business itself, eg the business owns a CA computer, which executes the CA software that collects CDR tickets and produces reports.

1.1.1 PBX and CA are within the Enterprise and are Co-Located

When the PBX and CA software package are co-located, the CDR data is typically produced by the PBX switch and transmitted to the CA software package via a direct serial connection. Since the CDR data is typically produced in real-time, eg at the completion of each call, the data is sometimes transmitted through an intermediate unit, referred to as a Buffer box, which provides intermediate storage. If the CA computer has crashed or is off-line for some reason, the intermediate storage in the buffer box assures that CDR data will not be lost – when the CA software comes back on-line, it can poll the Buffer box to retrieve the CDR data without loss of information. Figure 1 depicts the typical CA architectures using the direct connection method and the buffer box method.

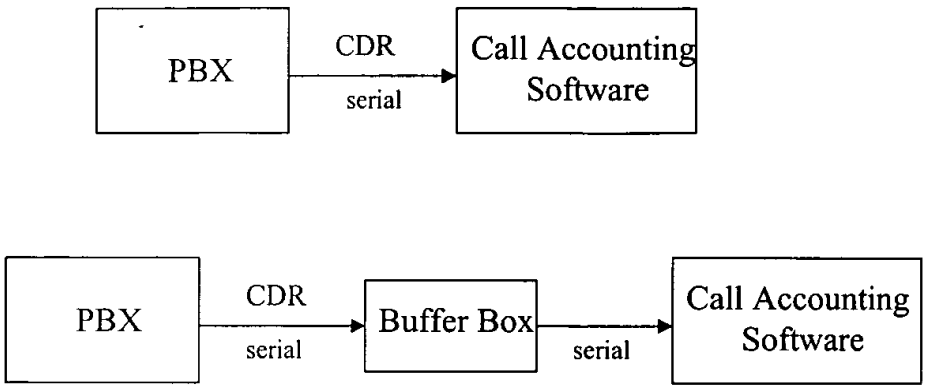

Figure 1: Direct Method and Buffer Box Method for Collecting CDR Data from PBX

1.1.2 PBX and CA are within the Enterprise and are Not Co-located

In many PBX installations, the CA system is positioned in a different location than the PBX system. For example, the telecom room containing the PBX system may not be physically comfortable for the administrator producing CDR reports, or there may be other physical space constraints which require that the PBX and CA software are separated by a large physical distance. Or the enterprise may have multiple branch offices, each having a separate PBX, with only a single CA software package located at the main location.

Modern buffer boxes support the ability to be polled via FTP using TCP/IP so that the CA software and the PBX can be located remotely. In this case, the data is transmitted from the PBX to the buffer box serially, and then the CA software, which may be located in a remote location, polls the buffer box using FTP and the CDR data is transmitted over the internal Enterprise LAN.

Note that when FTP is employed, a single CA software package can process the CDR data from multiple PBXs within the enterprise. For example, if an enterprise has its headquarters in New York with a branch office in Boston and Los Angeles, the CA software system could be located at the New York headquarters and could FTP the CDR data from buffer boxes located at the Boston and Los Angeles PBX systems. Buffer box architectures depicting the transmission of CDR data via FTP polling are depicted in Figure 2.

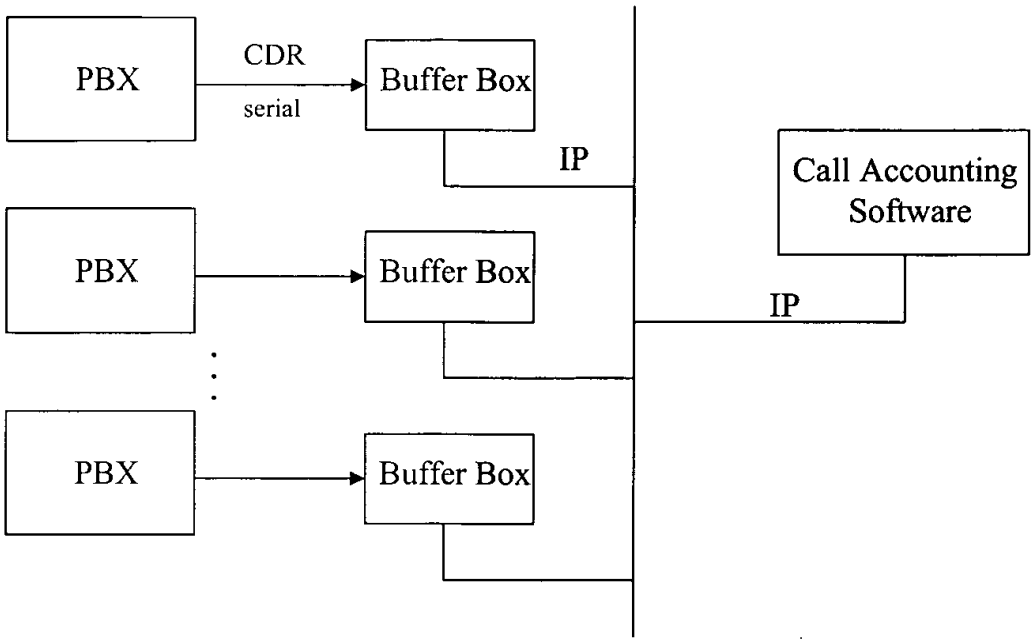

Figure 2: CDR Collection Based on Usage of Enterprise LAN. Call Accounting Software transfers CDR data from one or more PBXs via FTP over TCP/IP.

Buffer boxes typically also support dialup connections for remote access. In this case, rather than using the internal enterprise packet-switched network to transfer data, the PSTN network is used. The CA software package uses a modem to dial-up a remote buffer box and the CDR data is transmitted serially over the modem connection.

A variation of the FTP buffer box architecture is supported by the OmniPCX PBX switch. In this architecture, the CDR data is buffered internally within the OmniPCX on hard disc and can be polled via FTP by a CA software package located on the internal Enterprise LAN. Essentially, the OmniPCX eliminates the need for an external buffer box, since the real-time data is buffered and stored internally to the unit. A dial-up PPP connection is also supported when LAN access is not available and remote data acquisition must be performed via modem. A CA architecture depicting the usage of the OmniPCX is shown in Figure 3.

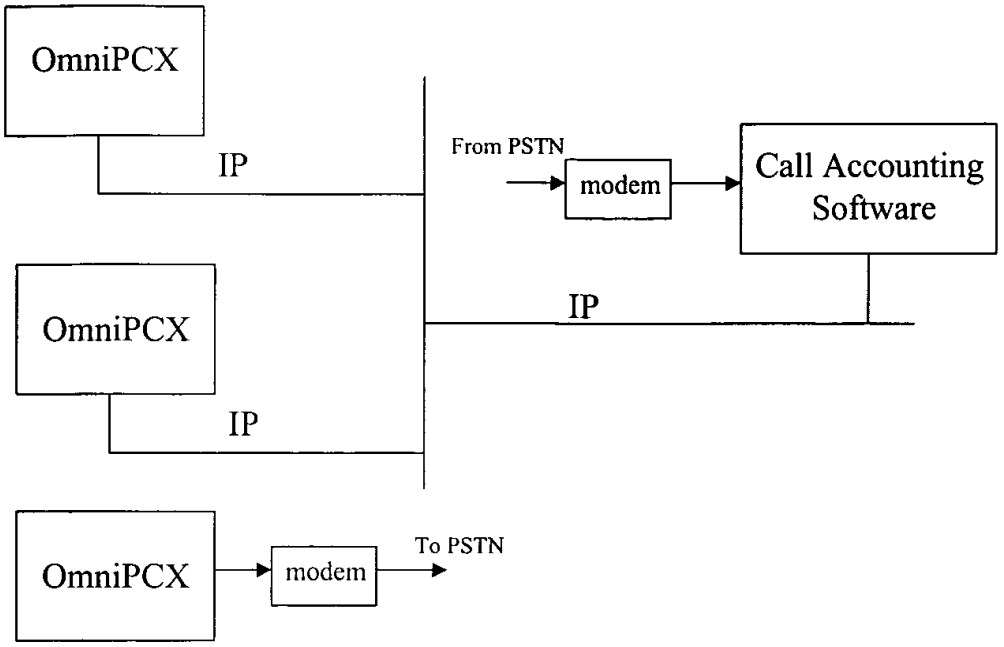

Figure 3: CDR Collection for Alcatel OmniPCXs. Data buffering and storage performed internally to the OmniPCX. CDR data collected via FTP over IP or via modem connection to/from PSTN.

1.2 Non-Enterprise-Resident Call Accounting:

In some cases, an enterprise may choose to outsource its Call Accounting functionality. In this case, an external service bureau owns the entire infrastructure required to produce the call accounting reports, and the enterprise pays a monthly or annual fee to receive various reports via email or Web access. Service Bureaus have been in existence for at least ten years, and in some cases provide a convenient alternative to Enterprises who do not wish to own and maintain their own Call Accounting computers, tariffs and databases. Service bureaus who provide access to Call Accounting reports are now called Call Accounting Application Service Providers, or CA-ASPs.

1.2.1 CA-ASP CDR retrieval via Dial-Up Connections

In order for a CA-ASP to provide reports to its multiple customers, it must be able to retrieve the CDR data from each of its customers' PBXs. Typically, this is performed using a nightly dial-up connection to the buffer box at each PBX location. The telephone call provides a secure, reliable means for accessing the stored CDR data at each location. However, the costs associated with placing these long-distance calls can be excessive. These costs, incurred by the CA-ASP are typically charged back to the enterprise. Figure 4 depicts this solution.

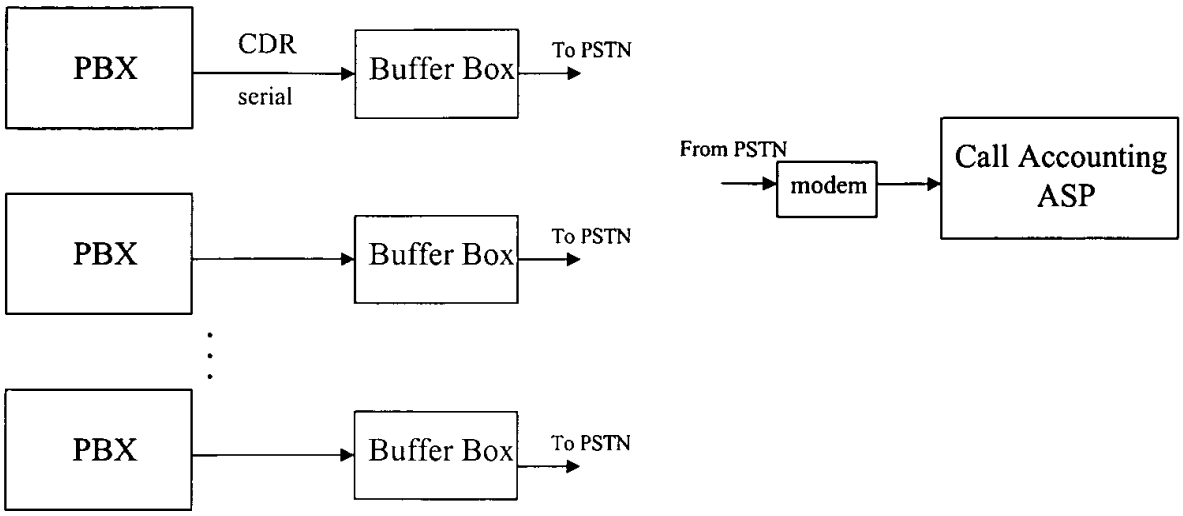

Figure 4: Call Accounting ASP transfers CDR data by making a long-distance call to each buffer box, and then transferring serial data over modem link. Telephone access is expensive and the data rate is relatively low.

1.2.2 CA-ASP CDR Retrieval via Buffer Box FTP over the Internet

In fact, most modern ASPs which provide other non-Call Accounting types of services to enterprises do **not** use dial-up connections. The connections between ASPs and Enterprises are made via the Internet. Since monthly access charges for frame relay connections between the Enterprise and the Internet Service Provider are typically fixed, there are no real direct costs associated with the connection between an Enterprise and a ASP when an Internet connection is used.

Since buffer boxes support FTP connection, the possibility exists for a CA-ASP to transfer the CDR from each remote PBX directly across the Internet. This architecture is depicted in Figure 5. However, most Enterprises are very reluctant to implement this architecture for security reasons – the CDR data contains an entire record of the Enterprise's calls. This data could be used to deduce private details of a company's business. Since buffer boxes do not typically encrypt the CDR data, any packet sniffing utility on the Internet could be utilized to derive the entire history of the calls and calling patterns on an Enterprise. Thus, CA-ASPs do **not** utilize the Internet to access the CDR buffer box data.

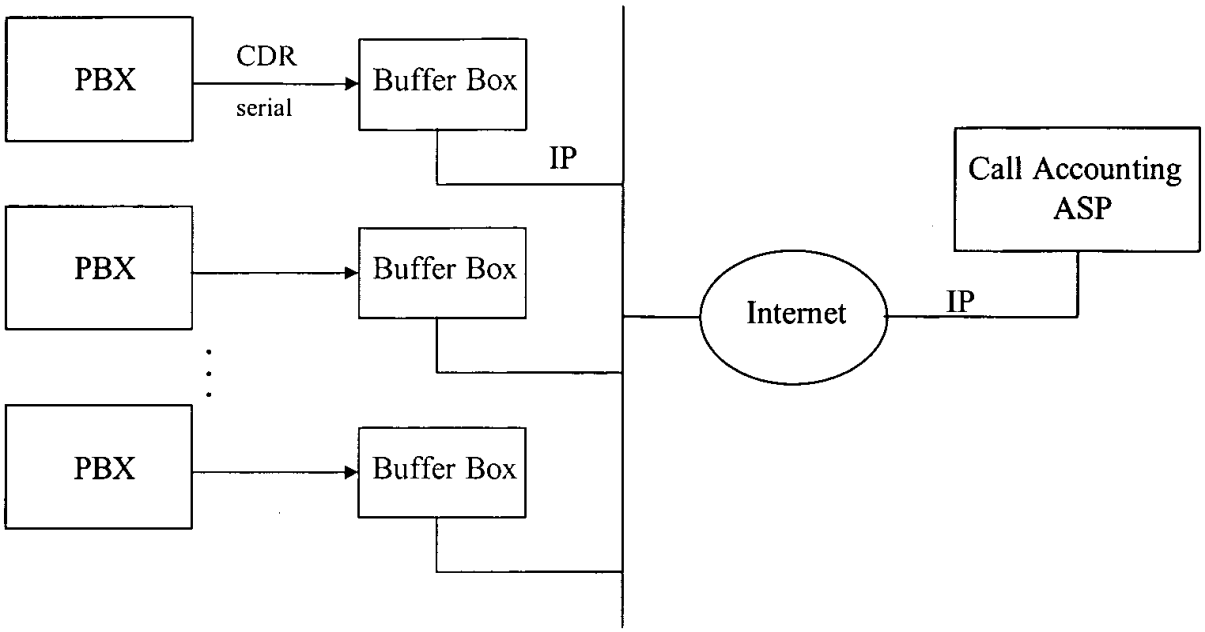

Figure 5: Call Accounting ASP transfers CDR data from one or more PBXs via FTP over TCP/IP across the Internet. This approach is very insecure as corporate telephone call information travels unprotected through various Internet routers.

1.2.3 Summary of the Limitations of Existing CA-ASP CDR Collection Techniques

Neither of the methods described in Sections 1.2.1 and 1.2.2 above are optimal for CA CDR collection. The CDR retrieval via direct dial-up can be expensive, especially if the CA-ASP is a global service provider located in a different country. The CDR retrieval method via FTP over the Internet is insecure and potentially compromises the business communications details of an Enterprise. As more and more Enterprises turn to CA-ASPs as an alternative to owning and maintaining their own computers, CA software, the importance of developing an alternative solution to the problem of CA-ASP CDR collection increases.

2.0 Summary of Problem Being Addressed by This Patent

Develop a means by which a CA-ASP can obtain CDR data from multiple PBXs over the Internet in a secure, reliable and cost-effective manner.

3.0 Summary of the Patent: Use of the Intelligent Ticket Collector (ITC)

The problem can be solved through the use of a device referred to as an Intelligent Ticket Collector (ITC) as depicted in Figure 6. The ITC is envisioned as a software application running on a general-purpose PC. The PC could be shared for other Enterprise uses. A dedicated hardware ITC unit is also envisioned.

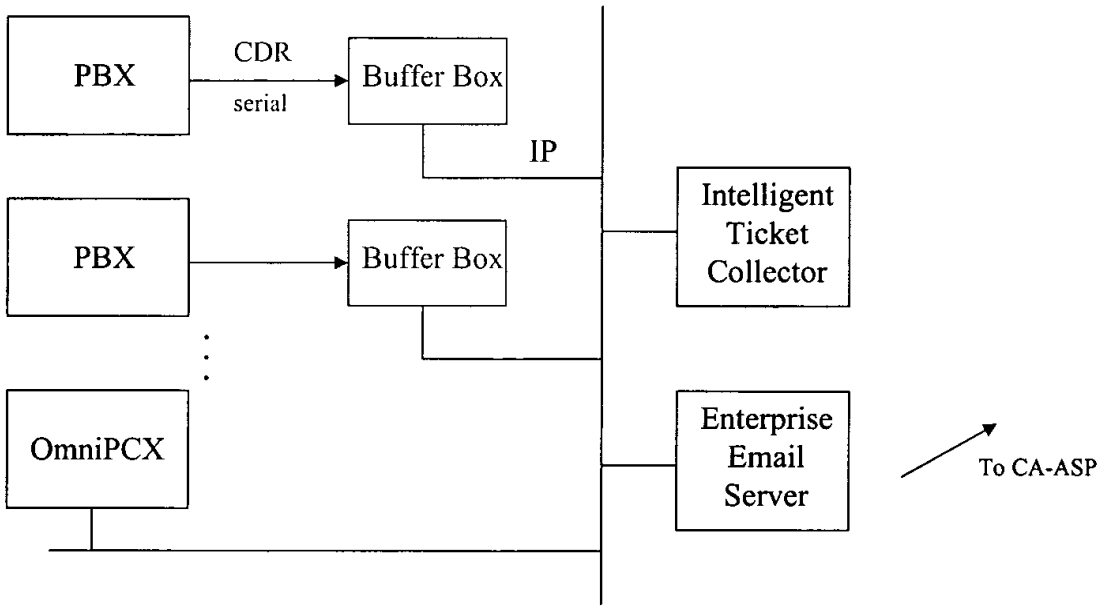

Figure 6: The Intelligent Ticket Collector (ITC) collects data from one or more buffer boxes or OmniPCXs, encrypts the data, and periodically emails the results to a CA-ASP. The CA-ASP decrypts and processes the CDR data. Reports are then made available through https or via secure email sent back to the Enterprise. The method eliminates the PSTN or direct Internet connection between the CA-ASP and the Enterprise.

One ITC is located within each Enterprise. The ITC collects data from buffer boxes within the Enterprise via FTP. In the case that the ITC is also accessing an OmniPCX, the FTP collection occurs directly to the OmniPCX and not through a buffer box. The collection of CDR data by the ITC is secure since the internal Enterprise network is protected from external access via corporate firewalls.

After collecting the CDR data on a periodic basis, the CDR data is encrypted using a standard one-way or-two way encryption algorithm. For example, a simple script running within the ITC application encrypts the collected data with the CA-ASP public key, using PGP, or a another encryption package.

After the encryption is performed, the ITC emails the encrypted CDR data to the CA-ASP. Note that emailing overcomes the security risks associated with the CA-ASP logging into to, or FTPing from a PC, located on the Enterprise LAN. The CDR data transfer between the Enterprise and the CA-ASP occurs via periodic secure email.

The ITC method is a push-based data transfer scheme, which differs from conventional pull-based data transfer schemes used by CAs and CA-ASPs.

This data transfer method overcomes both cost limitation associated with the direct dial-up method described in Section 1.2.1, and the security limitation associated with the FTP connection over the Internet, described in Section 1.2.2.

Upon receipt of the encrypted email from an Enterprise which has previously subscribed to a CA-ASP services, the CA-ASP decrypts the CDR data using its private key, and performs the CDR processing described in Section 1. Results are stored in the CA-ASP's database.

CA-ASP reports can be generated in several ways. First, pre-defined reports can be generated by the CA-ASP, encrypted with the Enterprise's public key and re-sent back to the Enterprise via email. The Enterprise then decrypts each report using its private key. Email scripts at both the CA-ASP and the Enterprise could automate the encryption/decryption process. Alternatively, the reports can be made available via the Web via an https connection. In the second method, Enterprise users with an appropriate password could view reports within a browser connected to the CA-ASP's secure Web server. This form of report access and generation is used by conventional CAs and conventional CA-ASPs.

3.1 Extensions of the Idea

3.1.1 Usage of the ITC to Send Voice Switch Information and Data Switch Information to a CA-ASP

Current CA software functionality is being extended to provide information about data usage as well as phone usage. For example, it may of interest to an Enterprise to better understand how its employees are using the Internet, or IP traffic summaries for various subnets or individual PCs within the Enterprise. CA functionality is currently being extended to provide this type of information and CA-ASPs are emerging to provide summary reports of this type of information.

The first extension of this patent is to use the ITC to send both voice switch connection information and data switch connection to a CA-ASP. In this extension, the ITC accesses individual data switches or IP-resident traffic collectors on the Enterprise WAN, and encrypts and emails the data, as described above.

3.1.2 Embedding the ITC within the PBX

A second extension of the patent is to embed the ITC within the PBX itself. For example, in the case of a software-based PBX system such as the OmniPCX, a simple internal Unix script can be written which periodically accesses internally stored CDR data, encrypts it, and emails it to a CA-ASP. In this way, the entire operation of sending the CDR information in a secure cost-effective manner is built-in to the functionality of the OnniPCX. Each OmniPCX perdiodically encrypts its own CDR data and emails it off to the CA-ASP address. No other external devices or software is needed as each OmniPCX is responsible for encrypting and emailing its own CDR data on a periodic basis. Similarly, the ITC could be embedded within a data switch so that encrypted reports are periodically email to an application service provider.

3.1.3 Incorporating Other Functionality within the ITC

Since the ITC is envisioned as software, it is possible to incorporate additional functionality within it, such as fraud alert and other alarm generation conditions. Using this approach, it is possible to redistribute some of the functionality between the ITC and the CA-ASP. For example, tariff management, automatic report generation, and directory updating could be managed at the CA-ASP while real-time alarm monitoring and alert generation could be managed by the ITC. In this case, the ITC is responsible for real-time operations, while the CA-ASP is responsible for more batch-oriented operations.

4.0 Summary

A novel method for collecting CDR data from one or more PBXs or OmniPCXs within an Enterprise has been described. The method is based on use of the Intelligent Ticket Collector (ITC). The ITC transfers data within the Enterprise via FTP, and then encrypts the data using a standard encryption algorithm. The encrypted results are then emailed to a CA-ASP. The CA-ASP processes the CDR tickets and stored the results within its database. Reports can be made available from the CA-ASP via https or via encrypted reports which are emailed back to the Enterprise. The method substantially reduces the costs and data transfer time associated with PSTN dial-up connections, and eliminates the security risks associated with FTP transfer via the Internet.